Controlled Quantum Secret Sharing

Chi-Yee Cheung*
Institute of Physics, Academia Sinica
Taipei, Taiwan 11529, Republic of China

We present a new protocol in which a secret multiqubit quantum state $|\Psi\rangle$ is shared by n players and m controllers, where $|\Psi\rangle$ is the encoding state of a quantum secret sharing scheme. The players may be considered as field agents responsible for carrying out a task, using the secret information encrypted in $|\Psi\rangle$, while the controllers are superiors who decide if and when the task should be carried out and who to do it. Our protocol only requires ancillary Bell states and Bell-basis measurements.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Mn
Keywords: quantum secret sharing, quantum cryptography, quantum information

Cryptography is the art and science of concealing a secret message from unauthorized parties. At present the most widely used cryptographic system is the RSA public-key protocol invented by Rivest, Shamir, and Adleman in 1978 [1]. However the security of this protocol is not proven, other than the fact the it is very hard to crack with our present knowledge of mathematics and technology.

The idea of quantum cryptography was first proposed in the 1970's by Wiesner [2]. In recent years, the field of quantum key distribution(QKD) has found many fruitful applications of quantum information theory [3]. Moreover, secure distributions of secret cryptographic keys have been demonstrated in and outside scientific laboratories [4, 5, 6, 7]. The first provably secure QKD protocol was constructed in 1984 by Bennett and Brassard [8] using polarized single photons. Quantum entanglement assisted QKD was first proposed by Ekert in 1991 [9]. Since then, many other QKD protocols have appeared in the literature.

In 1979 Blakely [10] and Shamir [11] introduced the notion of secret sharing as a means of safeguarding cryptographic keys. The idea is as follows. Suppose Alice wants to send a secret message to a remote location, and she has a choice of sending it to either agent Bob or agent Charlie. In order to reduce the risk of possible leakage and misuse of the message, it is often safer for her to split the message into two shares and send them to Bob and Charlie separately, such that either one alone has absolutely no knowledge of the message. Bob and Charlie can reconstruct the original secret message if and only if they cooperate with each other. More generally, in a so-called (k, n)-threshold scheme, the secret is divided into n shares, such that any k of those shares can be used to reconstruct the secret, while any set of less than k shares contains absolutely no information about the secret at all.

Quantum secret sharing (QSS) refers to the implementation of the secret sharing task outlined above using quantum mechanical resources. Hillery *et al.* [12] and Karlsson *et al.* [13] were the first to propose QSS protocols using respectively three-particle Greenberger-Horne-Zeilinger (GHZ) states and two-particle Bell states. Apart from quantum sharing of classical secrets, the idea has also been generalized to the sharing of secret quantum information [12, 13, 14], which is often referred to as "quantum state sharing" (also QSS). We shall mainly be concerned with this notion of QSS in this paper. Some recent theoretical works in this area can be found in Refs. [15, 16, 17, 18, 19, 20, 21]. On the experimental side, a (2,3) threshold QSS protocol has been demonstrated in the continuous variable regime [22]. QSS using pseudo-GHZ states has been reported earlier [23]. Recently, a three-party QSS scheme has also been demonstrated via four-photon entangled states [24].

Controlled quantum teleportation (CQT) is an extension of the original quantum teleportation protocol proposed by Bennett *et al.* [25] in 1993. The idea is to allow parties other than the receiver to have control over the successful completion of a teleportation process. In the first CQT protocol proposed by Karlsson *et al.* [26], an arbitrary single qubit state is teleported to two receivers using a GHZ state, such that only one of them can reconstruct the quantum state using classical information provided by the other. Recently quantum teleportation with multiparty control has also been proposed [27, 28, 29], in which the receiver can fully recover the quantum state if all of the controllers cooperate by communicating the outcomes of their measurements to the receiver. Yang *et al.* [27] and Zhang *et al.* [28] considered the controlled teleportation of a

*Electronic address: cheung@phys.sinica.edu.tw

multiqubit product state, and Deng *et al.* [29] a two-qubit entangled state. Furthermore controlled probabilistic teleportation of one- and two-qubit states has also been studied lately [30, 31]. Recent experimental works on quantum teleportation can be found in Refs. [32, 33, 34, 35].

Most of the discrete variable QSS protocols proposed in the literature are of the (n, n)-threshold type [12, 13, 16, 17, 18, 19, 20]. A (2,3)-threshold scheme using qutrits can be found in Ref. [14]. In the continuous variable regime, general (k, n)-threshold schemes are possible using optical interferometry [21, 36]. Typically shares of quantum information are distributed by teleportation or entanglement swapping via Bell or GHZ states established between the sender and the players. In ordinary QSS, after the completion of the distribution process, the fate of the secret quantum information is entirely left to the players. For example, in a (k, n)-threshold scheme, any k players may come together anytime, extract the quantum secret and use it to execute a certain task. This situation may not be desirable in many real world situations, especially when it is crucial that the extraction of the secret information (or the initiation of the subsequent actions) requires authorization from higher offices. For such cases, it is desirable to have a secret sharing protocol where it is impossible for the players to extract the secret information (even if all of them agree to cooperate) before obtaining authorization from superiors which we shall call "controllers".

In this paper, we propose a new protocol which may be viewed as a hybrid of QSS and CQT. We consider the following situation. The dealer Alice has a N-qubit state $|\Psi_{1\ldots N}\rangle$ which encrypts a secret quantum information $|\xi\rangle$, and it is to be shared by $n \le N$ players ($\mathcal{B}_1,\ldots,\mathcal{B}_n$) and $m \le 2N$ controllers ($\mathcal{C}_1,\ldots,\mathcal{C}_m$). $|\Psi_{1\ldots N}\rangle$ can be the encoding state of any secret sharing scheme, and we shall not specify it explicitly here. After the shares are properly distributed, successful reconstruction of the quantum secret $|\xi\rangle$ depends on two conditions: (1) At least m^* controllers must agree to release the classical information they hold (m^* depends on how the classical shares are distributed; see below), and (2) a set of at least k players must collaborate to perform a joint operation on the qubits they possess. Such a protocol may be termed "controlled quantum secret sharing" (CQSS).

It is easy to see that CQSS reduces to ordinary QSS if all the controllers make public the classical information they hold. Therefore the encoding state $|\Psi_{1\ldots N}\rangle$, together with its access structure, must satisfy the theorems on QSS obtained in Refs. [14, 15]. The existence of controllers in CQSS adds another dimension to ordinary QSS. In order to reconstruct the secret quantum information in CQSS, it is not sufficient that a minimum number of players agree to cooperate−they must first obtain authorization from the controllers. Note that the players and the controllers play asymmetric roles in a CQSS scheme: Namely the controllers hold no quantum shares, therefore their role is not to reconstruct the quantum secret themselves, but to control when it should be done and which players are assigned to do it. In QSS, there could also be asymmetry between the power of different players [14, 15], and this feature can be retained in CQSS in the access structure of the encoding state $|\Psi_{1\ldots N}\rangle$. CQSS protocols are useful in secure quantum communication networks. They are also useful in the real world situation where the players are field agents responsible for carrying out a certain task, using the secret information encrypted in $|\Psi_{1\ldots N}\rangle$, and the controllers are superiors who decide if and when the task should be carried out and who to do it.

Most proposals for multiparty QSS [12, 13, 14, 16, 17] and teleportation [26, 27, 29, 30, 31] with multiparty control require ancillary entangled states and/or collective measurements involving three or more qubits. In some cases the number of involved qubits increases with the N or m, making them difficult to implement by current technologies. In contrast, the CQSS scheme to be presented below requires only Bell-basis measurements and ancillary Bell states which are much easier to produce and purify.

The first step of the protocol is to divide $|\Psi_{1\ldots N}\rangle$ into n equal shares and distribute them to the n players. This can be achieved by entanglement swapping (or teleportation) as shown in Ref. [37]. The procedure is conceptually quite simple and we reproduce it below. To begin with, we define the four Bell states:

$$|\phi^{\pm}_{\mu\nu}\rangle = \frac{1}{\sqrt{2}}\Big(|0_\mu\rangle|1_\nu\rangle \pm |1_\mu\rangle|0_\nu\rangle\Big), \tag{1}$$

$$|\varphi^{\pm}_{\mu\nu}\rangle = \frac{1}{\sqrt{2}}\Big(|0_\mu\rangle|0_\nu\rangle \pm |1_\mu\rangle|1_\nu\rangle\Big), \tag{2}$$

where the singlet state $|\phi^{-}_{\mu\nu}\rangle$ is also known as the Einstein-Podolsky-Rosen (EPR) state. We assume that the Alice shares at least one EPR $|\phi^{-}_{\mu_i\nu_i}\rangle$ with each player $\mathcal{B}_i$, so that the total number of EPR states shared between them is N. Similarly she shares at least one EPR state $|\phi^{-}_{\alpha_i\beta_i}\rangle$ with each controller $\mathcal{C}_i$, and the total number is $2N$. It is to be understood that qubits $\{\mu_i\}$ and $\{\alpha_i\}$ belong to Alice, qubits $\{\nu_i\}$ and $\{\beta_i\}$ belong

respectively to the players and controllers. We first show how to distribute (or teleport) qubit-1 of $|\Psi_{1\ldots N}\rangle$ to $\mathcal{B}_1$, as we shall see the procedure can be easily generalized to include other qubits. The state $|\Psi_{1\ldots N}\rangle$ can always be cast in the form,

$$|\Psi_{1\ldots N}\rangle = a|0_1\rangle|\Phi_{2\ldots N}\rangle + b|1_1\rangle|\Phi'_{2\ldots N}\rangle, \tag{3}$$

where $|a|^2+|b|^2=1$, and $|\Phi_{2\ldots N}\rangle$ and $|\Phi'_{2\ldots N}\rangle$ are normalized states of $(N-1)$ qubits. Then we can write the product of $|\Psi_{1\ldots N}\rangle$ and $|\phi^-_{\mu_1\nu_1}\rangle$ as

$$\begin{aligned}|\Psi_{1\ldots N}\rangle|\phi^-_{\mu_1\nu_1}\rangle = \frac{1}{2}\Big[&|\varphi^+_{1\mu_1}\rangle\Big(a|1_{\nu_1}\rangle|\Phi_{2\ldots N}\rangle - b|0_{\nu_1}\rangle|\Phi'_{2\ldots N}\rangle\Big)\\ &+ |\varphi^-_{1\mu_1}\rangle\Big(a|1_{\nu_1}\rangle|\Phi_{2\ldots N}\rangle + b|0_{\nu_1}\rangle|\Phi'_{2\ldots N}\rangle\Big)\\ &- |\phi^+_{1\mu_1}\rangle\Big(a|0_{\nu_1}\rangle|\Phi_{2\ldots N}\rangle - b|1_{\nu_1}\rangle|\Phi'_{2\ldots N}\rangle\Big)\\ &- |\phi^-_{1\mu_1}\rangle\Big(a|0_{\nu_1}\rangle|\Phi_{2\ldots N}\rangle + b|1_{\nu_1}\rangle|\Phi'_{2\ldots N}\rangle\Big)\Big].\end{aligned} \tag{4}$$

Therefore a Bell-basis measurement by Alice on the pair of qubits $(1,\mu_1)$ will entangle $\mathcal{B}_1$'s qubit-ν_1 to the inactive group $(2,\ldots,N)$, such that the resulting N-qubit state depends on the outcome of Alice's measurement. Comparing with Eqs. (3), we see that if Alice informs $\mathcal{B}_1$ of the outcome, then by a local unitary transformation on qubit-ν_1, $\mathcal{B}_1$ can rotate the state of the N-qubit group $(\nu_1,2,\ldots,N)$ to $|\Psi_{\nu_1,2,\ldots,N}\rangle$, which is exactly what we started out with except that Alice's qubit-1 has been replaced by $\mathcal{B}_1$'s qubit-ν_1. The required unitary operators for the four possible outcomes $(|\varphi^+\rangle, |\varphi^-\rangle, |\phi^+\rangle, |\phi^-\rangle)$ are respectively $(\sigma_z\sigma_x,\ \sigma_x,\ \sigma_z,\ I)$, where

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{5}$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{6}$$

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|. \tag{7}$$

Notice that the above procedure is entirely general, in the sense that it is independent of the state of the inactive qubits $(2,\ldots,N)$. Accordingly it can be repeated on the other qubits until all of them are distributed to the players $(\mathcal{B}_1,\ldots,\mathcal{B}_n)$.

Upon completing the distribution process, Alice would have made N Bell-basis measurements (one for each qubit in $|\Psi_{1\ldots N}\rangle$), and obtained N Bell states, $\{|\psi^1\rangle,\ldots,|\psi^N\rangle\}$, where $|\psi^i\rangle \in \{|\phi^-\rangle, |\phi^+\rangle, |\varphi^-\rangle, |\varphi^+\rangle\}$. Hence there is a one-to-one correspondence between the qubits in $|\Psi_{1\ldots N}\rangle$ and the Bell states in the list $|\psi^1\rangle,\ldots,|\psi^N\rangle$. Each Bell state corresponds to two bits of classical information; for instance we may assign

$$|\phi^-\rangle \to 00, \quad |\phi^+\rangle \to 01, \tag{8a}$$

$$|\varphi^-\rangle \to 10, \quad |\varphi^+\rangle \to 11. \tag{8b}$$

In an ordinary QSS scheme, the Bell-state information is given to the players, so that they know what unitary transformations to apply to their qubits in order to recover the original state $|\Psi\rangle$. In contrast, for the CQSS protocol being considered here, Alice distributes the Bell-state information to the controllers $(\mathcal{C}_1,\ldots,\mathcal{C}_m)$ instead. She could do it quantum mechanically by teleporting the Bell states to the controllers using the same method described above. However it is simpler to just send the corresponding classical information as follows. Suppose Alice wants to send two bits (x,y) to $\mathcal{C}_i$ with whom she shares a pair of EPR states $|\phi^-_{\alpha_i\beta_i}\rangle$ and $|\phi^-_{\alpha'_i\beta'_i}\rangle$. From

$$\begin{aligned}|\phi^-_{\alpha_i\beta_i}\rangle|\phi^-_{\alpha'_i\beta'_i}\rangle = \frac{1}{2}\Big(&|\varphi^+_{\alpha_i\alpha'_i}\rangle|\varphi^+_{\beta_i\beta'_i}\rangle - |\varphi^-_{\alpha_i\alpha'_i}\rangle|\varphi^-_{\beta_i\beta'_i}\rangle\\ &-|\phi^+_{\alpha_i\alpha'_i}\rangle|\phi^+_{\beta_i\beta'_i}\rangle + |\phi^-_{\alpha_i\alpha'_i}\rangle|\phi^-_{\beta_i\beta'_i}\rangle\Big),\end{aligned} \tag{9}$$

we see that a Bell-basis measurement by Alice on qubits α_i and α'_i will leave the (β_i,β'_i) pair in one of the Bell states on $\mathcal{C}_i$'s side. Moreover the resulting Bell states on both sides are random but identical. Hence by the convention given in Eq. (8), Alice and $\mathcal{C}_i$ can obtain a pair of random bits (x',y') by independently performing a Bell-basis measurement on qubits (α_i,α'_i) and (β_i,β'_i) respectively. After that Alice can announce the two-bit

information $(x \oplus x', y \oplus y')$ (modulo 2) over a public channel, and $\mathcal{C}_i$ will be able to decode the secret bits (x, y) since he knows (x', y').

It is interesting to note that, instead of giving the two-bit information of a Bell state to one controller as described above, Alice could also choose to split the Bell state and have it shared by two controllers. Again this can be done by following the same procedure described earlier for the distribution of $|\Psi_{1\ldots N}\rangle$. In this case, the two controllers involved must cooperate to make a join Bell-basis measurement on their qubits in order to identify the Bell state they share. Moreover if one of the controllers does not cooperate, then the other one can get absolutely no information about the Bell state [42]. Consequently, each individual controller has no complete control over the release of the corresponding two-bit information. This option may be useful in circumstances where some controllers are of lower rank than others. This concludes the specification of our CQSS protocol.

Consider the simplest case where each player receives one qubit, and each controller one set of two-bit Bell-state information (*i.e.*, $n = m = N$). If any k controllers release their two-bit information, then the k players holding the corresponding qubits can collaborate to extract the secret information $|\xi\rangle$. Hence the minimum number of consenting controllers is $m^* = k$ in this case. Obviously if all the controllers agree to release the information they hold, then any authorized set of k players can extract the secret. If one of the controllers withholds his two-bit information, then knowledge about the corresponding qubit is completely hidden from the players. This can be seen from Eq. (4). Let the two-bit information corresponding to the distribution of qubit-1 be withheld, then the state of the N qubits $(\nu_1, 2, \ldots, N)$ is an equal mixture of the four possible outcomes as shown in Eq. (4). The corresponding density matrix is given by

$$\begin{aligned} \rho'_{N} &= \frac{1}{2}\, I_{\nu_1} \Big(|a|^2 |\Phi_{2\ldots N}\rangle\langle\Phi_{2\ldots N}| + |b|^2 |\Phi'_{2\ldots N}\rangle\langle\Phi'_{2\ldots N}| \Big), \\ &= \frac{1}{2}\, I_{\nu_1} \mathrm{Tr}_1 |\Psi_{1\ldots N}\rangle\langle\Psi_{1\ldots N}|, \end{aligned} \tag{10}$$

where I_{ν_1} is the identity matrix for qubit-ν_1. Clearly ρ'_{N} contains absolutely no information about qubit-1 in the original state $|\Psi_{1\ldots N}\rangle$. Hence if more than $(n-k)$ controllers withhold their information, the quantum secret $|\xi\rangle$ is sealed, even if all the players agree to cooperate.

In other situations where $n = N$ but $m < N$, some controllers may receive more than one set of Bell-state information (two bits). Then a controller holding more than $(n-k)$ sets would have veto power over the recovery of $|\xi\rangle$. It follows that if everyone receives more than $(n-k)$ sets, the recovery of $|\xi\rangle$ would require unanimous consent from all the controllers. In the special case where Alice keeps all the Bell-state information home, then she becomes the sole controller who can decide not only when to extract the secret information, but also which players are assigned to do so. Finally, if Alice discloses all the Bell state information to the players, then the result is an ordinary QSS scheme.

If $n = 1$, then CQSS reduces to the controlled teleportation of $|\Psi_{1\ldots N}\rangle$ with m controllers. Recently two CQT schemes with multiparty control have been proposed by Yang *et al.* [27] and Zhang *et al.* [28]. Both schemes considered only the controlled teleportation of a product state of N qubits, whereas our scheme can teleport an arbitrary N-qubit entangled state. The scheme of Ref. [27] requires an ancillary multiqubit entangled state, which is difficult if not impossible to implement when the number of qubits or controllers becomes large. Ref. [28] also employs only ancillary Bell states, and Alice transmits her measurement results to the controllers via a public channel using pre-established secret keys. In our case Alice could split a Bell state and have it shared by two different controllers; this option may be useful in certain circumstances, but it is not available in Refs. [27, 28] or other CQT schemes.

As with all entanglement based quantum protocols, the security of our scheme depends crucially on the quality of the quantum entanglement connections between Alice and the receivers (players and controllers). An important advantage of this type of schemes is that the set-up, purification, and checking of the shared EPR states can all be done prior to and independent of the scheme itself [38, 39, 40, 41]. In the CQSS protocol being considered here, Alice can conduct additional security checking during the distribution process by randomly inserting a number of decoy states $|\theta_j\rangle$, with $|\theta_j\rangle \in \{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$ for example. With M decoy qubits, the state to be distributed becomes

$$|\Psi'_{1\ldots N+M}\rangle = |\Psi_{1\ldots N}\rangle \prod_{j=1}^{M} |\theta_j\rangle, \tag{11}$$

At the conclusion of the distribution process, Alice identifies the decoy qubits and asks the players to measure them in appropriate bases and report the results. Checking against her own record for discrepancies, Alice can detect the existence of eavesdroppers. With appropriate number of decoys, the chance of an eavesdropper escaping detection can be made as small as desired. Similarly Alice can check for eavesdropping activities between herself and the controllers.

From the above discussions, it is clear that in order to implement our CQSS protocol, the sender Alice must first share N EPR states with the $n \leq N$ players, and $2N$ EPR states with the $m \leq 2N$ controllers. To distribute the the quantum shares to the players, Alice needs to make N Bell-basis measurements. A maximum of $2N$ Bell-basis measurements are required to send the Bell state information to the controllers (N measurements if she sends through classical channels only). Therefore, apart from classical communications, the whole distribution process requires $3N$ shared EPR states and $2N-3N$ Bell-basis measurements. Needless to say, extra resources would be needed if decoy qubits are employed. Typically, each decoy qubit would add one EPR state and one Bell-basis measurement to the resources requirement given above.

In summary we have presented in this paper a new protocol which we call “controlled quantum secret sharing (CQSS)”. In this protocol, the encoding state $|\Psi_{1\ldots N}\rangle$ is shared by n players and m controllers. After the completion of the distribution process, further action is to be initiated by the controllers by disclosing the classical information they hold, then an authorized set of players can proceed to extract the secret information as in ordinary secret sharing schemes. We recap the procedure as follows:

1. The dealer Alice possesses a N-qubit state $|\Psi_{1\ldots N}\rangle$ which encodes a secret quantum information $|\xi\rangle$. In addition she shares a total of N EPR states with $n \leq N$ players $\{\mathcal{B}_1,\ldots,\mathcal{B}_n\}$, and $2N$ EPR states with $m \leq 2N$ controllers $\{\mathcal{C}_1,\ldots,\mathcal{C}_m\}$.

2. Alice divides $|\Psi_{1\ldots N}\rangle$ into n shares, and distributes them to the players by entanglement swapping (or teleportation) [37]. In the process, she obtains N Bell states from the required Bell-basis measurements. Each Bell state corresponds to two bits of classical information. Normally Alice divides the Bell state information into m groups and transmits them to the controllers through encrypted classical channels. However if necessary Alice could also split any Bell state and have it shared by two different controllers.

In real world applications, the players may be considered as field agents responsible for carrying out a task, using the secret information encrypted in $|\Psi_{1\ldots N}\rangle$, and the controllers are superiors who decide if and when the task should be carried out and who to do it. Our protocol requires only ancillary EPR states and Bell-basis measurements, so that it is relatively simple to implement.

[1] R. L. Rivest, A. Shamir, and L. M. Adleman, Commun. ACM **21**, 120 (1978).
[2] S. Wiesner, SIGACT News **15**, 78 (1983).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, J. Cryptology **5**, 3 (1992).
[5] A. Muller, H. Zbinden, and N. Gisin Europhys. Lett. **33**, 335 (1996).
[6] G. Ribordy, J. Brendel, J-D. Gautier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2001).
[7] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).
[8] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processings, Bangalore, India* (IEEE, New York, 1984), p.175.
[9] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[10] G. R. Blakely, in *Proceedings of the AFIPS National Computer Conference, New York, 1979* (AFIPS Press, Montvale, NJ, 1979), Vol. 48, p. 313.
[11] A. Shamir, Commun. ACM **22**, 612 (1979).
[12] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[13] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[14] R. Cleve, D. Gottesman, and H. -K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[15] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[16] Y. Li, K. Zhang, and K. Peng, Phys. Lett. A **324**, 420 (2004).
[17] F. -G. Deng and H. -Y. Zhou, arXiv:quant-ph/0504158.
[18] L. -Y. Hsu, Phys. Rev. A **68**, 022306 (2003).
[19] Z. J. Zhang, J. Yang, Z. X. Man, and Y. Li, Eur. Phys. J. D **33**, 133 (2005).

[20] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[21] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).
[22] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[23] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[24] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, C. Y. Lu, C. Z. Peng, T. Yang, J. W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
[25] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[26] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998).
[27] C. -P. Yang, S. Han, Phys. Lett. A **343**, 267 (2005).
[28] Z. -J. Zhang and Z. -X. Man, Phys. Lett. A **341**, 55 (2005).
[29] F. -G. Deng, C. -Y. Li, Y. -S. Li, H. -Y. Zhou, and Y. Wang, Phys. Rev. A **72**, 022338 (2005).
[30] F. Yan and D. Wang, Phys. Lett. A **316**, 297 (2003).
[31] T. Gao, Commun. Theo. Phys. **42**, 223 (2004).
[32] J. A. W. van Houwelingen, A. Beveratos, N. Brunner, N. Gisin, and H. Zbinden, arXiv:quant-ph/0604211.
[33] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, Phys. Rev. Lett. **92**, 047904 (2004).
[34] Y. H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
[35] J. W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).
[36] T. Tyc, D. J. Rowe, and B. C. Sanders, J. Phys. A **36**, 7625 (2003).
[37] C. Y. Cheung, arXiv:quant-ph/0507069.
[38] C. -P. Yang and G. -C. Guo, Phys. Rev. A **59**, 4217 (1999).
[39] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[40] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[41] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[42] Alice could also choose to do it classically by splitting the two-bit information instead. However, in this case, even if one of controllers does not cooperate, the other still knows something about the Bell state.